S.No	Problem Statement ID	Problem Statement Name	Domain
16	CT-CS - 03	Passwordless Authentication	Corporate Sec

Description:

The **Passwordless Authentication System** is a secure and user-friendly method for accessing corporate systems and applications without relying on traditional passwords. Instead of passwords, the system uses advanced authentication methods such as biometric verification (fingerprint, face recognition), magic links, hardware tokens, or one-time codes sent via email or mobile devices.

This approach enhances security, reduces the risk of password-related breaches, and improves the user experience by eliminating the need to remember or manage complex passwords.

Objectives:

1. **Strengthen Security:**
    - Eliminate vulnerabilities associated with stolen, weak, or reused passwords.
2. **Simplify User Experience:**
    - Provide employees with a seamless and efficient way to access corporate systems.
3. **Prevent Data Breaches:**
    - Reduce the risk of phishing, brute force attacks, and credential stuffing.
4. **Enable Modern Authentication:**
    - Support advanced security protocols like FIDO2 and WebAuthn for robust corporate security.
5. **Improve Productivity:**
    - Minimize time spent on password resets and troubleshooting authentication issues.

Expectations:

1. **Secure Access Control:**
    - Replace traditional passwords with biometric authentication, hardware tokens, or magic links for accessing corporate resources.
2. **Flexible Integration:**
    - Integrate seamlessly with corporate identity and access management (IAM) systems.
3. **Scalability:**
    - Support large-scale implementation across departments, systems, and devices.
4. **Compliance:**
    - Align with corporate security policies and regulatory standards for authentication.

Expected Results:

1. **Reduced Security Risks:**
    - Minimize the threat of password-related attacks such as phishing and credential theft.
2. **Enhanced User Convenience:**
    - Provide employees with faster and easier access to systems without compromising security.
3. **Improved Corporate Security Posture:**
    - Strengthen overall security by adopting a modern, passwordless approach.
4. **Cost Savings:**
    - Lower IT support costs by reducing password reset requests and related helpdesk activities.